UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,696	01/27/2000	Takashi Shinzaki	000043	1253

23850 7590 12/31/2003

ARMSTRONG, KRATZ, QUINTOS, HANSON & BROOKS, LLP
1725 K STREET, NW
SUITE 1000
WASHINGTON, DC 20006

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/31/2003

4

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/492,696	SHINZAKI ET AL.	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The abstract of the disclosure is objected to because the abstract exceeds the limitation of 150 words. Correction is required. See MPEP § 608.01(b).

2. Claim 20 is objected to because of the following informalities:

(1) The word "measn" on line 26 of page 95 and all on page 96 should have been "means". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis (US 6,181,803 B1).

a. *Referring to claim 1:*

i. Davis teaches:

(1) a biometric information input unit inputting biometric information **[i.e., a biometric device 120 (e.g., as shown in Figure 1, a biometric scanner of facial or hand geometries, iris patterns, voice synthesizer) includes an input source (e.g., lens, scanner, microphone, etc.) that routes data to a biometric processor 200 having cryptographic functionality contained within the biometric device 120 (column 3, lines 51-52 and lines 59-62)];**

(2) an extraction unit extracting biometric feature information from the input biometric information **[i.e., as shown in Figure 1, the biometric processor 200 captures a data clip of desired data (e.g., facial geometries or other characteristics of a user 140 requesting access to the node) that obtains from biometric device 120 (column 3, lines 62-65)]**;

(3) an estimation unit estimating matching precision of the extracted biometric feature information **[i.e., as shown in Figure 1, the biometric processor 200 further processes the data clip locally therein before sending at least one "secure" message to the PC 110 to remain accessible or shut-down (column 3, lines 65-67). Ultimately, the processing performed by the processing unit 220 may extend to include the actual comparison of pre-stored master characteristics with the processed data clip to determine whether or not to grant the user access to the node (column 5, lines 22-26)]**;

(4) a request unit requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained **[i.e., for the sake of clarity, the selected biometric characteristics (from the data capture circuit 210, that is "a request unit ") will be described as visual physical characteristics (e.g., iris patterns, retina patters, finger prints, facial geometries, etc.), while it is contemplated that non-visual characteristics of the user (e.g., voice patterns, data entry patterns, etc.) may be used for authentication or identification purposes, whereas the pre-stored data does not match is inherently provided (column 4, lines 46-52)]**;

(5) an authentication information input unit inputting the authentication information **[i.e., as shown in Figure 2, the processor unit 220, that is "an authentication information input unit"]**;

(6) a biometric feature information registration unit preliminarily storing registered biometric feature information **[i.e., as shown in Figure 1, biometric processor 200, that is "a biometric feature information registration unit", captures a data clip of desired data (column 3, lines 62-63)]**;

(7) an authentication information registration unit preliminarily storing additional registered authentication information **[i.e., as shown in Figure 2, the data capture circuit 210, that is "an authentication information registration unit" for "storing additional registered authentication information"];**

(8) a biometric feature information matching check unit having a matching check between the extracted biometric feature information and the registered biometric feature information **[i.e., as shown in Figure 2, the processor unit 220, that is "a biometric feature information matching check unit"];**

(9) an authentication information matching check unit having a matching check between the input authentication information and the registered authentication information **[i.e., as shown in Figure 2, the processor unit 220, that is "an authentication information matching check unit"];** and

(10) a determination unit computing matching precision by combining a matching check result about biometric feature information with a matching check result about additional authentication information, and determining based on a computation result whether or not a user is authenticated **[i.e., as shown in Figure 2, the processor unit 220, that is "a determination unit" for "computing matching precision"].**

b. *Referring to claim 2:*

i. Davis further teaches:

(1) wherein said request unit requests password information as the authentication information, said authentication information input unit inputs the password information, said authentication information registration unit preliminarily stores registered password information as the registered authentication information, and said authentication information matching check unit has a matching check between the input password information and the registered password information **[i.e., "request unit requests password information as the authentication information" is considered to include in the data capture circuit 210 whereby the non-visual characteristics of the user (e.g., voice patterns, data entry patterns,**

that is "password information", etc.) may be used for authentication or identification purposes (column 4, lines 50-52)].

c. *Referring to claim 3:*

i. Davis further teaches:

(1) wherein said request unit comprises a setting unit setting a number of digits of password information required to obtain the predetermined matching precision, and requesting an input of the set number of digits of password information **[i.e., "a setting unit" is considered to include in the data capture circuit 210].**

d. *Referring to claim 4:*

i. Davis further teaches:

(1) wherein said number of digits is set based on the matching precision estimated by said estimation unit, and said authentication information matching check unit has a matching check between the input password information and a predetermined part of the registered password information **[i.e., "number of digits is set based on the matching precision estimated by said estimation unit" is considered to include in biometric processor 200].**

e. *Referring to claim 5:*

i. Davis further teaches:

(1) wherein said determination unit inputs authentication information stored in a medium **[i.e., "authentication information" is considered to be stored in the memory element 222, as shown in Figure 2].**

f. *Referring to claims 6 and 10:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

g. *Referring to claim 7:*

i. Davis further teaches:

(1) wherein said request unit requests an input of other biometric information of a same type as the biometric information used in estimating matching precision, and said biometric information input unit inputs other biometric

information of the same type at the request **[i.e., as shown in Figure 2, the data capture circuit 210, that is for "requesting an input of other biometric information of a same type as the biometric information used in estimating matching precision"].**

h. *Referring to claim 8:*

i. Davis further teaches:

(1) wherein said biometric information input unit inputs fingerprint information as biometric information, and requests an input of fingerprint information about a finger different from a finger used in fingerprint information in a matching check for estimating the matching precision **[i.e., a biometric device 120 (e.g., as shown in Figure 1, a biometric scanner of facial or hand geometries or finger prints, iris patterns, voice synthesizer) includes an input source (e.g., lens, scanner, microphone, etc.) that routes data to a biometric processor 200. The processing performed by the processing unit 220 may extend to include the actual comparison of pre-stored master characteristics with the processed data clip to determine whether or not to grant the user access to the node (column 5, lines 22-26)].**

i. *Referring to claim 9:*

i. Davis further teaches:

(1) wherein said request unit requests an input of biometric information of a different type from biometric information used in estimating matching precision, and said biometric information input unit inputs biometric information of a different type **[i.e., as shown in Figure 2, the data capture circuit 210, that is for "requesting an input of biometric information of a different type from the biometric information used in estimating matching precision"].**

j. *Referring to claim 11:*

i. Davis further teaches:

(1) wherein said biometric information relates to one of fingerprint information, iris information, voiceprint information, retina blood vessel distribution information, signature information, face image information, and DNA

information **[i.e., the selected biometric characteristics will be described as visual physical characteristics (e.g., iris patterns, retina patters, finger prints, facial geometries, etc.) (column 4, lines 46-49)]**.

k. *Referring to claim 12:*

i. Davis further teaches:

(1) a client device **[i.e., the node 110 of Figure 1]** in a client-server type authentication system, comprising:

(a) a biometric information input unit inputting biometric information **[i.e., a biometric device 120 of Figure 1];**

(b) an extraction unit extracting biometric feature information from the input biometric information **[i.e., a biometric processor 200 of Figure 1];**

(c) an estimation unit estimating matching precision of the extracted biometric feature information **[i.e., a processing unit 220 of Figure 2 may extend to include the actual comparison of pre-stored master characteristics with the processed data clip to determine whether or not to grant the user access to the node (column 5, lines 22-26)];**

(d) a request unit requesting an input of additional authentication information when it is estimated that predetermined matching precision cannot be obtained **[i.e., for the sake of clarity, the selected biometric characteristics (from the data capture circuit 210, that is "a request unit ") will be described as visual physical characteristics (e.g., iris patterns, retina patters, finger prints, facial geometries, etc.), while it is contemplated that non-visual characteristics of the user (e.g., voice patterns, data entry patterns, etc.) may be used for authentication or identification purposes, whereas the pre-stored data does not match is inherently provided (column 4, lines 46-52)];**

(e) an authentication information input unit inputting the authentication information **[i.e., as shown in Figure 2, the processor unit 220, that is "an authentication information input unit"];**

(f) a generation unit generating matching check data by combining the extracted biometric feature information with the input authentication information **[i.e., as shown in Figure 2, the processor unit 220, that is "a generation unit" for "generating matching check data"]**; and

(g) a communications unit transmitting the matching check data to a server to have a matching check between the generated matching check data and registered information **[i.e., as shown in Figure 1, the biometric device 120, that is "a communications unit", comprises the data capture circuit 210 including a pixel capture array 211 and control logic 212 controlling the pixel capture array 211. The control logic 212 digitizes biometric characteristics of the user and transmits the digitized version of the biometric characteristic to the processing unit 220 (column 4, lines 55-57)]**.

l. *Referring to claim 13:*

i. Davis further teaches:

(1) wherein said matching data generation unit described in the matching data at least one of the extracted biometric feature information, type information about the input authentication information, and format information about the matching data **[i.e., normally, for a user authentication biometric system, its biometric device (wherein "matching data generation unit" is considered to include in this device) captures a data clip and transmits the data clip to a computer operating as a database through a signal line in a non-encrypted format. The computer processes the data clip, searches for pre-stored "master" characteristics of the individual requesting access to the node who has previously identified oneself through voice, data input and other input means, compares the data clip to the pre-stored master characteristics, and grants access to a node or an area if certain features of the data clip match those of the pre-stored master characteristics contained in the computer (column 1, lines 42-53)]**.

m. *Referring to claim 14:*

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

ii. Davis further teaches:

(1) a communications unit receiving biometric feature information and additional authentication information from a client **[i.e., as shown in Figure 1, biometric device 120, that is "a communications unit"].**

n. *Referring to claim 15:*

i. This claim has limitations that is similar to those of claims 10, 12, and 14, thus it is rejected with the same rationale applied against claims 10, 12, and 14 above.

o. *Referring to claim 16:*

i. This claim has limitations that is similar to those of claim 12, thus it is rejected with the same rationale applied against claim 12 above.

ii. Davis further teaches:

(1) a communications unit transmitting the registration data to a server to register the generated registration data. **[i.e., as shown in Figure 1, biometric device 120, that is "a communications unit" for "transmitting the registration data to a server to register the generated registration data"].**

p. *Referring to claim 17:*

i. This claim has limitations that is similar to those of claims 14 and 15, thus it is rejected with the same rationale applied against claims 14 and 15 above.

q. *Referring to claim 18:*

i. Davis further teaches:

(1) a database unit managing a type of registered information stored corresponding each piece of identification information **[i.e., as shown in Figure 2, the node may communicate with a remotely located source (e.g., a centralized database, that is "a database unit") to receive master characteristics of the user downloaded from the remotely located source (column 5, lines 43-46)];**

(2) a retrieval unit retrieving a type of registered information corresponding to identification received from a client **[i.e., referring still to Figure 2, the processing unit 220, that is "a retrieval unit" for "retrieving a type of registered information corresponding to identification received from a client"];** and

(3) a request unit requesting the client to input matching information corresponding to the retrieved type **[i.e., referring still to Figure 2, the data capture circuit 210, that is "a request unit" for "requesting the client to input matching information corresponding to the retrieved type"].**

r. *Referring to claims 19 and 20:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Burger et al (US 6,219,439 B1) discloses a biometric authentication system is provided which includes a dual input reader, the inputs consisting of stored physiological data of a user on a chip disposed on a smart card, and a fingerprint scan for comparison against the stored data (see abstract).

b. Gennaro et al (US 6,317,834 B1) discloses a method of performing biometric authentication of a person's identity including a biometric template prior to storing it in a biometric database (see abstract).

c. Houvener (US 6,424,249 B1) discloses the biometric access authority information input through biometric scanner and the physical appearance of person identified by identification terminal, are compared with that stored in remote database and accordingly access authority is granted to user (see abstract).

d. Baumann (US 6,104,922) discloses a method and apparatus for authenticating subscriber units (30) and users (25) in a communications system includes a communications node (200) which receives biometric information describing a user (25), and measures an RF signature of the subscriber unit (30).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
December 19, 2003

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100